EXHIBIT A

SUPREME COURT STATE OF NEW YORK
COUNTY OF QUEENS

LORRELL DUMAY, DIAN DUMAY, and JODI WOLFSON, individually and on behalf of all others similarly situated, Plaintiffs -against- EPISCOPAL HEALTH SERVICES INC., Defendant.	Index No. _____ Summons Filed: September 11, 2019 **SUMMONS**

To the above-named Defendant:

You are hereby summoned and required to answer the attached complaint of the Plaintiffs in this action and to serve a copy of your answer upon the attorneys for the Plaintiffs at the address stated below.

If this summons was personally delivered to you in the State of New York, you must serve the answer within 20 days after such service, excluding the day of service. If this summons was not personally delivered to you in the State of New York, you must serve the answer within 30 days after service of the summons is complete, as provided by law.

If you do not serve an answer to the attached complaint within the applicable time limitation stated above, a judgment may be entered against you, by default, for the relief demanded in the complaint.

Plaintiffs designate Queens County as the place of trial.

The basis of venue is defendant Episcopal Health Services Inc.'s residence, which is in the County of Queens: 327 Beach 19th Street, Far Rockaway, New York 11691.

Dated: September 11, 2019

Respectfully Submitted,

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/Jeremiah Frei-Pearson*
Jeremiah Frei-Pearson
Todd S. Garber
John Sardesai-Grant
Andrew C. White
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
Tel.: (914) 298-3281
jfrei-pearson@fbfglaw.com
tgarber@fbfglaw.com
jsardesaigrant@fbfglaw.com
awhite@fbfglaw.com

PAUL M. SOD, ESQ.
337R Central Avenue
Lawrence, New York 11559
Tel.: (516) 295-0707
paulmsod@gmail.com

Attorneys for Plaintiffs and the Proposed Class

SUPREME COURT STATE OF NEW YORK
COUNTY OF QUEENS

LORRELL DUMAY, DIAN DUMAY, and JODI WOLFSON, individually and on behalf of all others similarly situated, Plaintiffs -against- EPISCOPAL HEALTH SERVICES INC., Defendant.	Index No. _____ Date Purchased: September 11, 2019 **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson, individually and on behalf of all other similarly situated persons, by and through their attorneys, Paul M. Sod and Finkelstein, Blankinship, Frei-Pearson & Garber, LLP, as and for their class action complaint against defendant Episcopal Health Services Inc., respectfully allege, upon their own knowledge or, where they lack personal knowledge, upon information and belief including the investigation of their counsel, as follows:

INTRODUCTION

1. Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson ("Plaintiffs") bring this class action lawsuit on behalf of themselves and all other similarly situated persons against defendant Episcopal Health Services, Inc. ("Defendant") as a result of its failure to safeguard and protect the confidential information of Plaintiffs and the other members of the Class -- including financial information (e.g., credit card numbers and bank account information), medical information, and other personal information (e.g., Social Security Numbers and dates of birth), and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information") -- in Defendant's custody, control, and care.

2. Plaintiffs were each patients at St. John's Episcopal Hospital ("St. John's"), which, upon information and belief, was owned by Defendant, for purposes of receiving medical treatment. As a condition to St. John's providing that medical treatment, the Plaintiffs were required to and did supply certain items of Sensitive Information to the Defendant -- including, but not limited, to their respective social security numbers, dates of birth, financial information, and other information.

3. Unbeknownst to Plaintiffs, Defendant did not have sufficient cyber-security procedures and policies in place to safeguard the Sensitive Information that Plaintiffs provided to Defendant. As a result, one or more of Defendant's employees email accounts were subject to unauthorized access, -- or "hacked" -- between August 28, 2018, and October 5, 2018 (the "Data Breach"). Plaintiffs and members of the proposed Class suffered damages as a result of the unauthorized disclosure of their Sensitive Information.

4. Plaintiffs assert causes of action sounding in common negligence, negligent hiring and training of employees, breach of fiduciary duty, implied contract, and delay in notification of the data breach, all arising from Defendant's failure to safeguard their Sensitive Information, and bring claims for consequential damages, injunctive relief, and punitive damages.

PARTIES

5. Plaintiff Lorrell Dumay is and was a resident of Queens County, New York, who has been a patient at St. John's and whose Sensitive Information was compromised in the Data Breach described herein.

6. Plaintiff Dian Dumay is and was a resident of Queens County, New York, who has been a patient at St. John's and whose Sensitive Information was compromised in the Data Breach described herein.

7. Plaintiff Jodi Wolfson is and was a resident of Queens County, New York, who has been a patient at St. John's and whose Sensitive Information was compromised in the Data Breach described herein.

8. Upon information and belief, defendant Episcopal Health Services Inc. is a religious corporation existing pursuant to the laws of the State of New York with its principal place of business in Far Rockaway, New York, within Queens County, New York.

9. The Defendant owns, operates, and controls St. John's, located in Far Rockaway, New York, and approximately ten satellite locations all within Queens or Nassau Counties.

JURISDICTION AND VENUE

10. This Court has jurisdiction over all causes of action asserted herein. Defendant is subject to the personal jurisdiction of this Court pursuant to CPLR 301.

11. Defendant has conducted and does conduct business in the State of New York, including through operation of the Facility.

12. Venue is proper in Queens County pursuant to CPLR 503(c) because Defendant maintains its principal place of business in Queens County.

THE SCOURGE OF DATA BREACHES

13. This action is brought in the midst of the ongoing onslaught of data breaches that plague the internet and computer era. In just the first six months of 2018, more than 4.5 Billion records (including medical, credit card and/or financial data, and other personally identifiable information) were breached or compromised.[1] That means that more than 25 million records

[1] https://www.cbronline.com/news/global-data-breaches-2018, last accessed May 7, 2019

were compromised or exposed in data breaches *every day*, or 291 records compromised or exposed *every second*.

14. The sheer number of victims and extent of data breaches is astounding. Here is a sampling of some of the bigger data breaches reported to date:

- Myheritage.com, a DNA ancestry company: 92,000,000 victims.[2]
- Equifax, one of the three major credit bureaus: 143,000,000 victims.[3]
- "MyFitnessPal" App, 150,000,000 victims.[4]
- Exactis.com, a leading compiler and aggregator of business and consumer data, 340,000,000 records, approximately 2/3 from consumers and 1/3 from businesses[5]
- Marriot Hotels, up to 500,000,000 people.[6]
- Yahoo.com, over 500,000,000 Yahoo! user accounts.[7]
- Verifications.io, an email verification site, 763,000,000 records.[8]
- Facebook, up to two billion accounts.[9]

---

[2] https://us.norton.com/internetsecurity-emerging-threats-myheritage-data-breach-exposes-info-of-more-than-92-million-user.html

[3] https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/need-know-equifax-data-breach/, last accessed May 2, 2019

[4] https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html

[5] https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/exactis-data-breach/

[6] https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach

[7] https://en.wikipedia.org/wiki/Yahoo!_data_breaches

[8] https://www.bankinfosecurity.com/breach-verificationsio-exposes-763-million-records-a-12158

[9] https://www.cbronline.com/news/global-data-breaches-2018, last accessed May 7, 2019

15. In the words of one leading internet magazine subcaptioned to an article on the most recent 540,000,000 Facebook accounts being compromised, "Don't expect news of these serious privacy fouls to stop anytime soon."[10]

16. One of the primary methods of accomplishing a data hack is through malware, defined by wikipedia.org as "any software intentionally designed to cause damage to a computer, server, client, or computer network.[11] One leading financial journal estimated that upwards of one million malware threats are created *every day*.[12]

DATA BREACHES OF MEDICAL PROVIDERS

17. Medical providers have been a primary target of hackers because of the rich cache of Sensitive Information which patients must disclose to their various medical providers.

18. A comprehensive study undertaken by the JAMA Network found that data breaches exposing medical records increased from 199 hacks in 2010 to 344 hacks in 2017, with the corresponding number of compromised medical records increasing from 5.9 million to 176.3 million, respectively.[13]

19. The results of the JAMA Network study were presented in the following chart:[14]

---

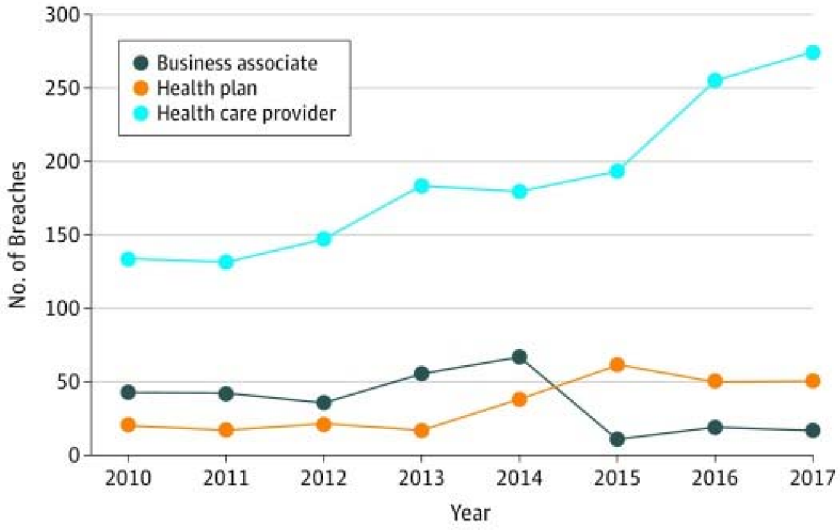
[10] https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html last accessed May 7, 2019

[11] https://en.wikipedia.org/wiki/Malware, last accessed on May 2, 2019

[12] https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

[13] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6233611/, last accessed May 2, 2019

[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6233611/bin/jama-320-1282-g001.jpg, last accessed May 2, 2019



Cumulative records breached, millions

Business associate	1.5	10.5	11.6	12.6	21.0	25.0	28.5	28.7
Health plan	3.6	3.7	4.0	4.1	6.2	109.1	110.0	110.4
Health care provider	0.8	5.0	6.3	12.1	14.1	20.5	32.7	37.2

20. Another authoritative study in 2016 found that data breaches at healthcare organizations were on the increase; that the organizations thought they were more vulnerable to data breach than other organizations; yet these organizations were unprepared to address new threats.[15] The study also found that healthcare organizations' biggest concern in cybersecurity was employee negligence, and that the majority of data breaches were caused by criminal acts.[16]

21. Medical provider data breaches continue unabated. The U.S. Department of Health and Human Services has created a "breach portal" where pursuant to section 13402(e)(4) of the HITECH Act, the HHS Secretary must post a list of breaches of unsecured protected

[15] https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1?q=library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1, cited in New York State Bar Association Journal, May 2019, p.15

[16] https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1?q=library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1, p. 3, 5

health information affecting 500 or more individuals.[17] As of May 2, 2019, the HHS breach portal showed that there were 132 hacks between January 3, 2019, and April 19, 2019, alone, affecting some 3,999,767 individuals.[18]

DATA BREACHES LEAD TO IDENTITY THEFT

22. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the hacker can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating and more.[19] A data hack can also result in the revelation of highly confidential and compromising information.[20]

23. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[21] As the GAO Report states, this type of identity theft is the most

---

[17] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[18] It is not known what correlation there is between the quantification of stolen data in the JAMA Network as "medical records" and the quantification of stolen data in the HHA Breach Portal as "individuals."

[19] *See* https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/ (last accessed May 7, 2019).

[20] *See, e.g.*, https://en.wikipedia.org/wiki/Ashley_Madison_data_breach (last accessed May 2, 2019).

[21] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 3, 2019).

harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

24. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[22]

25. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

26. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

27. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give

---

[22] *Id.* at 2, 9.

[23] *Id.* at 29 (emphasis added).

the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[24]

28. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Personal Information directly on various Internet websites making the information publicly available.

29. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

30. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value -- whereas a stolen social security number, on the other hand, only sells for $1."[26] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[24] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

[25] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited June 3, 2019).

[26] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 3, 2019).

DEFENDANT ALLOWED CRIMINALS TO OBTAIN PLAINTIFFS AND THE CLASS' SENSITIVE INFORMATION.

31. Emails of Defendant's employees were subject to "unauthorized access" between August 28, 2018, and October 5, 2018, resulting in criminals unlawfully obtaining patients' Social Security numbers, dates of birth, financial account information, medical history information, prescription information, medical record numbers, treatment or diagnosis information, and health insurance information or policy numbers (the "Data Breach").

DEFENDANT PROVIDED NOTICE TO PLAINTIFFS AND THE CLASS -- BUT LATE!

32. Defendant eventually notified Plaintiffs and members of the Class that its systems had been breached and that their Sensitive Information was compromised only in April 2019 -- some ten months after the first unauthorized access to the Class's emails in August 2018, some nine months after discovering the data breach in September 2018, and some eight months after allegedly stopping the data breach complained of herein.

33. Defendant utilized two methods to notify Plaintiffs and members of the Class of the Data Breach. First, Defendant's website added a page disclosing that its employees' emails were hacked and that critical patient information had been compromised (the "Web Notification").[27] For the convenience of the Court, a copy of the entire text of the Web Notification is annexed hereto as Exhibit A and is excerpted in pertinent part as follows:

> **What Happened?** On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third party forensic investigators, we determined that certain employee email accounts were subject to

[27] https://ehs.org/application/files/3015/4239/2982/Episcopal_Health_Services_-_Website_Notice_888.pdf, last accessed May 6, 2019

unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. On November 1, 2018, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals. The types of information contained within the potentially impacted emails are: Social Security number, date of birth, financial account information, medical history information, prescription information, medical record number, treatment or diagnosis information, and health insurance information or policy number. The types of information varied by individual.

Episcopal Health Services is not aware of any reported attempted or actual misuse of any personal information as a result of this event.

What is Episcopal Health Services doing in response to this incident? Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying and offering 12 months of complimentary credit monitoring to potentially affected individuals so that they may take further steps to best protect their personal information, should they feel it is appropriate to do so. We are also notifying any required federal and state regulators.

What should I do in response to this incident? Episcopal Health Services encourages you to remain vigilant against incidents of identity theft and fraud. You should review your account statements or your loved ones' account statements for suspicious activity. If you see any unauthorized charges, promptly contact the bank or credit card company. We also recommend reviewing your credit report for inquiries from companies that you have not contacted, accounts you did not open and debts on your accounts that you cannot explain.

What can I do to protect my information?

Monitor Your Accounts.

> *Credit Reports*. Episcopal Health Services encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.
>
> *Security Freeze* You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies . . . .
>
> * * * *
>
> As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies . . . .

34. Second, on April 16, 2019, Defendant sent a letters to Lorrell Dumay, Dian Dumay, and Jodi Wolfson advising each of them that their Sensitive Information had been subject to unauthorized access and had been compromised between August 28, 2018, and

October 5, 2018 (the "Letter Notifications"). Copies of the Letter Notifications are annexed hereto as Exhibits B, C, and D.[28]

35. The date of posting the Web Notification is not known but is reasonably assumed by Plaintiffs to have been on or about the date of the Letter Notifications, or April 16, 2019.

DEFENDANT'S ADMISSION OF NEGLIGENCE AND LIABILITY

36. Defendant had obligations created by HIPAA, promises made to patients like Plaintiffs and other Class Members, and based on industry standards, to keep the compromised Sensitive Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Sensitive Information to Defendant with the common sense understanding that Defendant, its employees, and any business partners to whom Defendant disclosed or entrusted the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

37. In the Web Notification and Letter Notifications (collectively, the "Breach Notifications"), Defendant admitted its own negligence when it wrote that the data breach resulted from the compromise and unauthorized access of "certain employee email accounts."

38. Defendant further admitted its own negligence in the Breach Notifications in that despite learning of suspicious activity in employee email accounts on September 18, 2018, it failed to take definitive steps to stop the unauthorized access of confidential information until October 5, 2018.

39. Defendant compounded the actual and potential harm arising from the Data Breach by not notifying the plaintiffs and other class members of the compromise of their

[28] Plaintiffs presume that Defendant sent a similar Letter Notification to all individuals whose Sensitive Information was exposed in the Data Breach.

personal information until April 2019, when the Breach Notifications were made. Defendant suggested in the Breach Notifications that Plaintiffs review account statements, monitor credit reports, and perhaps institute security freezes of their financial accounts to safeguard their financial well-being from harm arising from the disclosure of their Sensitive Information. Defendant's long and unjustified delay in notifying Plaintiffs and the Class that they were victims of the Data Breach will surely dilute any salutary effect that might come from these suggestions.

40. Defendant's security failure demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiffs' and the Class members' Sensitive Information;

c. Ensuring the confidentiality and integrity of electronic protected health information they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

41. Each Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information -- including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) a loss of privacy. The individual representative Plaintiffs and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identify theft and their attendant dangers for the rest of their lives because their dates of birth, Social Security numbers, medical information, and related personal information are in the hands of cyber-criminals.

DEFENDANT'S INADEQUATE RESPONSE TO THE DATA BREACH

42. Defendant's Breach Notifications stated that it had enhanced its cybersecurity by changing the log-in credentials of all employee email accounts, enhancing security controls, and implementing additional controls. No details were provided, and thus it cannot be determined from the Breach Notifications whether Defendant did any of the foregoing, or if it did, whether the enhancements were sufficient to prevent recurrences similar to the Data Breach.

43. As to the notification to the Plaintiffs and other victims of the Data Breach, the Breach Notifications stated that:

> *In an abundance of caution*, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

See, e.g., Ex. A (emphasis added).

44. Defendant's suggestion that it was notifying the Plaintiffs and other members of the Class of this data breach "in an abundance of caution" is dubious at best. GBL § 899AA(2) specifically provides that every business is required to notify any New York resident of any breach of the person's personal data "in the most expedient time possible and without unreasonable delay".[29] The Breach Notifications, coming some ten months after the initial intrusions, some nine months after Defendant became aware of the intrusions, and some eight months after Defendant contends that they were eliminated, were not made in the most expedient time possible, nor without unreasonable delay.

45. The untimely Breach Notifications also included an offer from Defendant of one year of free credit monitoring, fraud consultation, and identity theft restoration services through a third party provider. Defendant, however, offered an unreasonably short window of opportunity to claim these services, with victims of the Data Breach needing to claim these services by July 19, 2019, or be closed out. In addition, one year of credit counseling services is insufficient, given that Plaintiffs' and the Class members' risk of identity theft will continue throughout their life.

46. Conspicuously absent from the Breach Notifications is any offer of compensation for out-of-pocket losses which the Class has and foreseeably will sustain -- including, but not limited to, time spent to rectify any and all harms that resulted from the Data Breach. Plaintiffs

[29] GBL §899-AA(2) in pertinent part provides, "Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay…"

and members of the Class have suffered financial loss, including but not limited to lost opportunity costs for the time and efforts necessary to remedy the harm they suffered. Thus, Defendant's offer in the Breach Notifications fails to make Plaintiffs and the other members of the Class whole.

CLASS ALLEGATIONS

47. This action is brought on behalf of Plaintiffs and all similarly situated persons pursuant to Civil Practice Law and Rules 901, *et seq.* The Class is defined as:

> All persons whose Sensitive Information, provided to Defendant as part of their obtaining medical treatment at St. John's Episcopal Hospital or its satellite facilities, was exposed to unauthorized access by way of employee email accounts between August 28, 2018, and October 5, 2018.

48. Plaintiffs reserve the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

49. Plaintiffs are members of the Class.

50. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers, directors, and employees of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

51. This action seeks both injunctive relief and damages.

52. Plaintiffs and the Class satisfy the requirements for class certification for the following reasons:

53. **Numerosity of the Class.** At this time, Plaintiffs do not know the exact number of members of the Class, but the number is estimated to be at least in the hundreds, if not thousands. Therefore, the members of the Class are so numerous that their individual joinder is

impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

54. **Common Questions of Fact and Law.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant's data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;

b. Whether Defendant's data security systems prior to the Data Breach met industry standards;

c. Whether Plaintiffs' and other Class members' Sensitive Information was compromised in the Data Breach; and

d. Whether Plaintiffs and other Class members are entitled to damages as a result of Defendants' conduct.

55. **Typicality.** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

56. **Adequacy.** The Plaintiffs will fairly and adequately represent the Class on whose behalf this action is prosecuted. Their interests do not conflict with the interests of the Class.

57. Plaintiffs and their chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") and Paul M. Sod -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class

members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

58. **Superiority.** A class action is superior to any other available methods for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate so large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

59. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only St. John's patients, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures

unworkable or overly expensive. The identity of the Class members can be identified from Defendants' records, such that direct notice to the Class members would be appropriate.

60. In addition, Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or equitable relief with respect to the Class.

FIRST CAUSE OF ACTION

NEGLIGENCE IN THE HANDLING OF PLAINTIFFS' SENSITIVE INFORMATION

61. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

62. Defendant owed a duty to the Plaintiffs and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiffs' and Class members' Sensitive Information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over employee email accounts so as to prevent unauthorized access thereof.

63. Defendant owed a duty of care to the Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that email traffic adequately protected the Sensitive Information of the patients in its hospital and satellite facilities.

64. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between it and its patients, which is recognized by laws including, but not limited to, HIPAA. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Class from a data breach.

65. Defendant's duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendant is required to "reasonably protect" confidential data from "any

intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

66. In addition, Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

67. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Sensitive Information.

68. Defendant breached its common law, statutory, and other duties -- and thus, was negligent -- by failing to use reasonable measures to protect patients' Sensitive Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the Class members' Sensitive Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiffs' and the Class members' Sensitive Information;

d. failing to recognize in a timely manner that Plaintiffs' and the Class members' Sensitive Information had been compromised; and

e. failing to warn Plaintiff and other Class members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

69. Defendant owed a duty of care to the Plaintiffs and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

70. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

71. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

72. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information of the Plaintiffs and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate employee cyber-security training and email security protocols in place to secure Sensitive Information.

73. As a result of the foregoing, the Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of the Plaintiffs and the Class

which Plaintiffs and members of the Class were required to provide to Defendant as a condition to obtaining medical care at St. John's.

74. Plaintiffs and members of the Class reasonably relied on the Defendant to safeguard their information. and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiffs and members of the Class suffered and continue to suffer the consequences of the Data Breach.

75. Defendant's negligence was the proximate cause of harm to the Plaintiffs and members of the class. Indeed, Defendant admitted that it was the cause of the data breach.

76. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of the hospital's patients, the Plaintiffs' and Class members' Sensitive Information would not have been exposed to unauthorized access and stolen and they would not have suffered any harm.

77. However, as a direct and proximate result of Defendant's negligence, Plaintiffs and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiffs and members of the Class have been injured by, among other things; (1) the loss of the opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiffs' and the Class members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to

prevent, detect, and recover from identity and healthcare/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial and/or healthcare and/or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, healthcare or medical accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in the Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the data breach as a remainder of the Plaintiffs' and Class members' lives.

78. Plaintiffs and the Class seek consequential damages, punitive damages, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

NEGLIGENT HIRING AND TRAINING OF EMPLOYEES

79. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

80. Upon information and belief and based on the Breach Notifications, Plaintiffs' and the Class members' Sensitive Information was compromised through the actions of certain of its employees in their email accounts.

81. Defendant had a duty to adequately hire, train, and supervise its employees, including each and every employee whose email was the source of the disclosure of Sensitive Information of the Plaintiffs and the members of the Class.

82. The Data Breach complained of herein and the harm that befell the Plaintiffs and members of the Class was a result of the failure of the Defendant to adequately hire, train, and supervise its employees and/or by failing to or negligently hiring, training, and supervising its employees.

83. Defendant knew or reasonably should have known that its employees had a propensity for negligent behavior with respect to protecting Sensitive Information prior to the date of Data Breach yet still took unreasonable and insufficient actions to prevent the compromise of Plaintiffs' and the Class members' Sensitive Information, as alleged herein.

84. Accordingly, Defendant is liable to Plaintiffs and the Class for negligently hiring, retaining, and supervising employees that caused the data breach.

85. By reason of the foregoing, Plaintiffs and the Class members have been injured and suffered damages in an amount to be determined at trial, including, but not limited to, monetary damages and expenses for adequate and proper credit and identity theft monitoring and insurance, periodic credit reports, loss of privacy, and other ordinary, incidental, punitive and consequential damages, as well as attorney's fees to prosecute this action.

THIRD CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

86. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

87. The Plaintiffs and members of the Class provided Sensitive Information to the Defendant in connection with their obtaining needed medical treatments from St. John's or one of its satellite facilities and were required to provide their Sensitive Information as a condition of receiving medical treatment thereat.

88. Defendant would not have provided treatment to Plaintiffs, nor to any members of the Class had the Plaintiffs and members of the Class not provided various forms of Sensitive Information to Defendant -- including their social security numbers, dates of birth, financial information, health insurance information, and other privileged and confidential items of information.

89. Plaintiffs and members of the Class had no alternative and did not have any bargaining power with regards to providing their Sensitive Information. The Defendant required disclosure of Sensitive Information as a condition to rendering medical treatment, which the Plaintiff and members of the Class did.

90. When Plaintiffs and Class members paid money and provided their Sensitive Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

91. Defendant solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Sensitive Information to Defendant. In entering into such implied contracts, Plaintiffs and the Class assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant

would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

92. Plaintiffs and the Class would not have provided and entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

93. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

94. Defendant breached their implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

95. As a direct and proximate result of Defendant's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein

FOURTH CAUSE OF ACTION

BREACH OF FIDUCIARY DUTY

96. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

97. The Defendant collected Sensitive Information from the Plaintiffs and members of the class as part of the physician-patient relationship.

98. The relationship between the Defendant and the Plaintiffs and members of the class thus was a fiduciary relationship.

99. Plaintiffs and members of the class contend that this fiduciary relationship included a fiduciary duty to safeguard the Sensitive Information which Defendant insisted -- as a condition of medical treatment -- that the Plaintiff and members of the Class provide to the

Defendant. This duty required Defendant to ensure that the interests of Plaintiffs and members of the Class would be adequately protected both before and after the Data Breach.

100. As a result of Defendant's breach of its fiduciary duties, Plaintiffs and the members of the Class have suffered actual damages and prospective damages which are likely to arise.

101. Plaintiffs consequently demand judgment on behalf of themselves and the Class for breach of the Defendant's fiduciary duty and request equitable and/or injunctive relief alleviating the harms resulting from Defendant's breach of its fiduciary duties and/or prevent further harm from occurring..

FIFTH CAUSE OF ACTION

VIOLATION OF GENERAL BUSINESS LAW § 899-AA

102. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

103. Defendant became aware what it called "suspicious activity in employee email accounts" on September 18, 2018. After investigation, Defendant admitted that there were certain employee email accounts that were subject to unauthorized access between August 28, 2018, and October 5, 2018.

104. Despite the dates of the foregoing, the Defendant failed to provide notification to the Plaintiffs and members of the Class until April 16, 2019, when the Letter Notifications were sent out and when the Web Notification was posted.

105. Pursuant to General Business Law § 899-AA(2), the Defendant was obligated to provide disclosure to the victims of a data breach within "the most expedient time possible and without unreasonable delay…"

106. The Defendant, in delaying upwards of ten months to notify the Plaintiffs and members of the Class of the Data Breach violated General Business Law § 899-AA(2).

107. Plaintiffs demand damages from the Defendant for all damages that resulted from the delay in providing notification as required by law under General Business Law § 899-AA(2).

SIXTH CAUSE OF ACTION

VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

108. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

109. Defendant, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade, and commerce and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendant failed to enact adequate privacy and security measures to protect the Class members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendant failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Defendant knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendants knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information, including but not limited to duties imposed by HIPAA; and

e. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

110. As a direct and proximate result of Defendant's practices, Plaintiffs and other Class members suffered injury and/or damages, including, but not limited to, time and expenses

related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

111. The above unfair and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and other Class members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

112. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful.

113. Plaintiffs seeks relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial but will not be less than $50.00 per violation. *Id.*

114. Plaintiffs and Class members seek to enjoin the unlawful deceptive acts and practices described above. Each Class member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions, because, as detailed herein, Defendant will continue to fail to protect Sensitive Information entrusted to it.

115. Plaintiffs and Class members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

SEVENTH CAUSE OF ACTION

INJUNCTION – CPLR ARTICLE 63

116. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

117. Plaintiffs seek an injunction from this Court compelling Defendant to implement cyber-security policies and procedures equal to or better than industry standards.

118. As alleged herein, the failures of the Defendant to implement adequate cyber-security and email protocols has led to the compromise of the Sensitive Information Plaintiffs and members of the Class were required to provide as a condition of obtaining medical treatment from St. John's, resulting in irreparable harm.

119. Defendant remains in possession of the Sensitive Information of Plaintiffs and the Class. It is imperative that the Court intervene to assure that the Defendant takes all reasonable steps to protect that Sensitive Information lest there be another data breach at St. John's.

120. Plaintiffs and the Class have no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson demand judgment on behalf of themselves and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing the named Plaintiffs to be class representatives and the undersigned counsel to be class counsel;

b. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiffs and the Class appropriate relief, including actual damages, statutory damages, compensatory damages, and punitive damages on the First, Second, Third, Fourth, Fifth, and Sixth Causes of Action;

d. Awarding injunctive relief on the Seventh Cause of Action requiring the Defendant Episcopal Health Services Inc. to safeguard the Sensitive Information

of all persons providing Sensitive Information to the it as part of and as a condition of medical treatment;

e. Awarding Plaintiffs and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiffs and the Class their attorneys' fees and costs pursuant to CPLR 909 and other applicable laws, together with their costs and disbursements of this action; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs, individually and on behalf of the Class, demand a trial by jury as to all issues triable of right.

Dated: September 11, 2019

Respectfully Submitted,

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/Jeremiah Frei-Pearson*
Jeremiah Frei-Pearson
Todd S. Garber
John Sardesai-Grant
Andrew C. White
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
Tel.: (914) 298-3281
jfrei-pearson@fbfglaw.com
tgarber@fbfglaw.com
jsardesaigrant@fbfglaw.com
awhite@fbfglaw.com

PAUL M. SOD, ESQ.
337R Central Avenue
Lawrence, New York 11559
Tel.: (516) 295-0707
paulmsod@gmail.com

Attorneys for Plaintiffs and the Proposed Class

VERIFICATION

STATE OF NEW YORK)
) ss.:
COUNTY OF NASSAU)

I, Lorrell Dumay, being duly sworn depose and say:

1. I am a Plaintiff in the within action.

2. I have read the within Complaint and know the contents thereof; that the same is true to my own knowledge, except as to those matters therein stated to be upon information and belief, and that as to those matters, I believe it to be true.

Lorrell C. Dumay
Lorrell Dumay

Sworn to before me this
9 day of September, 2019

Notary Public
State of New York

PAUL M SOD
Notary Public, State of New York
No. 02SO4864010
Qualified in Nassau County
Commission Expires June 09, 2022

VERIFICATION

STATE OF NEW YORK)
) ss.:
COUNTY OF NASSAU)

I, Dian Dumay, being duly sworn depose and say:

1. I am a Plaintiff in the within action.

2. I have read the within Complaint and know the contents thereof; that the same is true to my own knowledge, except as to those matters therein stated to be upon information and belief, and that as to those matters, I believe it to be true.

Dian Dumay

Sworn to before me this
10 day of September, 2019

Notary Public
State of New York
DIANE DUMAY

DEBRA ZYLBERMINC
Notary Public, State of New York
Registration No. 01ZY6371658
Qualified in Queens County
My Commission Expires March 5, 2022

VERIFICATION

STATE OF NEW YORK)
) ss.:
COUNTY OF NASSAU)

I, Jodi Wolfson, being duly sworn depose and say:

1. I am a Plaintiff in the within action.

2. I have read the within Complaint and know the contents thereof; that the same is true to my own knowledge, except as to those matters therein stated to be upon information and belief, and that as to those matters, I believe it to be true.

Jodi Wolfson

Sworn to before me this
3 day of September, 2019

Notary Public
State of New York

PAUL M SOD
Notary Public, State of New York
No. 02SO4864010
Qualified in Nassau County
Commission Expires June 09, 2022

Exhibit A

NOTICE OF DATA PRIVACY EVENT

Episcopal Health Services recently discovered an incident that may affect the security of personal information of certain current and former patients. We take this incident very seriously and the confidentiality, privacy, and security of our information is one of our highest priorities.

What Happened? On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. On November 1, 2018, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals. The types of information contained within the potentially impacted emails are: Social Security number, date of birth, financial account information, medical history information, prescription information, medical record number, treatment or diagnosis information, and health insurance information or policy number. The types of information varied by individual.

Episcopal Health Services is not aware of any reported attempted or actual misuse of any personal information as a result of this event.

What is Episcopal Health Services doing in response to this incident? Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying and offering 12 months of complimentary credit monitoring to potentially affected individuals so that they may take further steps to best protect their personal information, should they feel it is appropriate to do so. We are also notifying any required federal and state regulators.

What should I do in response to this incident? Episcopal Health Services encourages you to remain vigilant against incidents of identity theft and fraud. You should review your account statements or your loved ones' account statements for suspicious activity. If you see any unauthorized charges, promptly contact the bank or credit card company. We also recommend reviewing your credit report for inquiries from companies that you have not contacted, accounts you did not open and debts on your accounts that you cannot explain.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. Episcopal Health Services encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission. **The Federal Trade Commission** can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

Questions regarding the incident should be directed to 1-866-775-4209, Monday through Friday from 9:00a.m. to 6:00 p.m. Eastern Time.

Exhibit B

ST. JOHN'S EPISCOPAL HOSPITAL
EPISCOPAL HEALTH SERVICES INC.

April 16, 2019

12 1 2803 **********AUTO**5-DIGIT 11691
LORRELL DUMAY
1037 GIPSON ST
FAR ROCKAWAY, NY 11691-2409

Re: Notice of Data Event

Dear Lorrell Dumay,

Episcopal Health Services is writing to advise you of a recent event that may impact the security of your personal information. While we are unaware of any actual or attempted misuse of the protected health information, we write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

What Happened? On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. This was a resource heavy review that took several months to complete. On February 26, 2019, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals, including you. However, the list of potentially affected individuals provided by the vendor did not include addresses for a large number of individuals and included many potential duplicates. Therefore, Episcopal Health Services was required to review its records to attempt to locate the missing addresses and remove potential duplicates. This process was completed on March 19, 2019.

What Information Was Involved? The email accounts subject to unauthorized access contained the following types of information relating to you: your name, date of birth, medical history information, treatment information/diagnosis, treating/referring physician/provider, medical record number, and health insurance information. Based upon available forensic evidence, Episcopal Health Services was able to confirm that your information was included within email accounts subject to unauthorized access but was unable to confirm whether the email containing your information was actually viewed by the unauthorized actor.

What We Are Doing. Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We are also notifying any required federal and state regulators.

As an added precaution, we are offering you access to 12 months of free identity monitoring services through Kroll. We encourage you to take advantage of these services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 19, 2019** to activate your identity monitoring services.*
Membership Number: **A29900048**

To receive credit services by mail instead of online, please call 1-833-231-3362. Additional information describing your services is included with this letter.

What You Can Do. You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud*. You can also enroll to receive the free services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-833-231-3362 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

We sincerely regret the inconvenience this incident causes for you. Episcopal Health Services remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

William Fedorich

William Fedorich
Vice President, General Counsel

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can

obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 12 Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Exhibit C

ST. JOHN'S EPISCOPAL HOSPITAL
EPISCOPAL HEALTH SERVICES INC.

April 16, 2019

12 1 2802 **********AUTO**5-DIGIT 11691
DIANE DUMAY
1037 GIPSON ST PH
FAR ROCKAWAY, NY 11691-2409

Re: Notice of Data Event

Dear Diane Dumay,

Episcopal Health Services is writing to advise you of a recent event that may impact the security of your personal information. While we are unaware of any actual or attempted misuse of the protected health information, we write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

What Happened? On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. This was a resource heavy review that took several months to complete. On February 26, 2019, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals, including you. However, the list of potentially affected individuals provided by the vendor did not include addresses for a large number of individuals and included many potential duplicates. Therefore, Episcopal Health Services was required to review its records to attempt to locate the missing addresses and remove potential duplicates. This process was completed on March 19, 2019.

What Information Was Involved? The email accounts subject to unauthorized access contained the following types of information relating to you: your name, medical history information, treating/referring physician/provider, and medical record number. Based upon available forensic evidence, Episcopal Health Services was able to confirm that your information was included within email accounts subject to unauthorized access but was unable to confirm whether the email containing your information was actually viewed by the unauthorized actor.

What We Are Doing. Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We are also notifying any required federal and state regulators.

As an added precaution, we are offering you access to 12 months of free identity monitoring services through Kroll. We encourage you to take advantage of these services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 19, 2019** to activate your identity monitoring services.*
Membership Number: **A29900045**

To receive credit services by mail instead of online, please call 1-833-231-3362. Additional information describing your services is included with this letter.

What You Can Do. You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud*. You can also enroll to receive the free services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-833-231-3362 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

We sincerely regret the inconvenience this incident causes for you. Episcopal Health Services remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

William Fedorich

William Fedorich
Vice President, General Counsel

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can

obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 12 Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Exhibit D

ST. JOHN'S EPISCOPAL HOSPITAL
EPISCOPAL HEALTH SERVICES INC.

April 16, 2019

46 1 10770 **********AUTO**5-DIGIT 11691
JODI WOLFSON
910 DINSMORE AVE APT 3G
FAR ROCKAWAY, NY 11691-4726

Re: Notice of Data Event

Dear Jodi Wolfson,

Episcopal Health Services is writing to advise you of a recent event that may impact the security of your personal information. While we are unaware of any actual or attempted misuse of the protected health information, we write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

What Happened? On September 18, 2018 Episcopal Health Services became aware of suspicious activity in employee email accounts. We immediately began an investigation to determine what happened and what information may have been affected. With the assistance of third-party forensic investigators, we determined that certain employee email accounts were subject to unauthorized access between August 28, 2018 and October 5, 2018. These email accounts were then reviewed to determine whether they contained any protected health or personal information. This was a resource heavy review that took several months to complete. On February 26, 2019, Episcopal Health Services determined that the accounts subject to unauthorized access contained protected health information of certain individuals, including you. However, the list of potentially affected individuals provided by the vendor did not include addresses for a large number of individuals and included many potential duplicates. Therefore, Episcopal Health Services was required to review its records to attempt to locate the missing addresses and remove potential duplicates. This process was completed on March 19, 2019.

What Information Was Involved? The email accounts subject to unauthorized access contained the following types of information relating to you: your name, date of birth, medical history information, treating/referring physician/provider, medical record number, health insurance information, and health insurance policy number. Based upon available forensic evidence, Episcopal Health Services was able to confirm that your information was included within email accounts subject to unauthorized access but was unable to confirm whether the email containing your information was actually viewed by the unauthorized actor.

What We Are Doing. Episcopal Health Services is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls to help protect employee email accounts from unauthorized access. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We are also notifying any required federal and state regulators.

As an added precaution, we are offering you access to 12 months of free identity monitoring services through Kroll. We encourage you to take advantage of these services. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 19, 2019** to activate your identity monitoring services.*
Membership Number: **A30064161**

To receive credit services by mail instead of online, please call 1-833-231-3362. Additional information describing your services is included with this letter.

What You Can Do. You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud*. You can also enroll to receive the free services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-833-231-3362 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

We sincerely regret the inconvenience this incident causes for you. Episcopal Health Services remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

William Fedorich

William Fedorich
Vice President, General Counsel

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can

obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 12 Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

----------X

LORRELL DUMAY, DIAN DUMAY, and JODI WOLFSON, individually and on behalf of all others similarly situated,,

Plaintiff,

-against-

EPISCOPAL HEALTH SERVICES INC.,

Defendants.

----------X

Index No. 715629/2019

NOTICE OF APPEARANCE

TO THE CLERK OF THIS COURT AND ALL PARTIES OF RECORD:

PLEASE TAKE NOTICE that Todd S. Garber of Finkelstein, Blankinship, Frei-Pearson & Garber, LLP located at 445 Hamilton Avenue, Suite 605, White Plains, NY 10601, telephone number (914) 298-3283, fax number (914) 908-6721 hereby enters an appearance in this matter on behalf of the Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson.

Dated: September 12, 2019

Respectfully submitted,

/s/ Todd S. Garber

Todd S. Garber
Finkelstein, Blankinship, Frei-Pearson & Garber, LLP
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Tel. (914) 298-3283
Fax. (914) 908-6721
Email: tgarber@fbfglaw.com

Counsel for Lorrell Dumay, Dian Dumay, and Jodi Wolfson.

CERTIFICATE OF SERVICE

I, Todd S. Garber, hereby certify that on September 12, 2019 caused the foregoing NOTICE OF APPEARANCE to be filed electronically in the above-captioned action via the Court's CM/ECF system, which caused electronic copies to be served on all counsel of record.

By: */s/ Todd S. Garber*

Todd S. Garber
Finkelstein, Blankinship, Frei-Pearson & Garber, LLP
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Tel. (914) 298-3283
Fax. (914) 908-6721
Email: tgarber@fbfglaw.com

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

----------X

LORRELL DUMAY, DIAN DUMAY, and JODI WOLFSON, individually and on behalf of all others similarly situated,,

Plaintiff,

-against-

EPISCOPAL HEALTH SERVICES INC.,

Defendants.

----------X

Index No. 715629/2019

NOTICE OF APPEARANCE

TO THE CLERK OF THIS COURT AND ALL PARTIES OF RECORD:

PLEASE TAKE NOTICE that John Sardesai-Grant of Finkelstein, Blankinship, Frei-Pearson & Garber, LLP located at 445 Hamilton Avenue, Suite 605, White Plains, NY 10601, telephone number (914) 298-3292, fax number (914) 908-6706 hereby enters an appearance in this matter on behalf of the Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson.

Dated: September 12, 2019

Respectfully submitted,

/s/ John Sardesai-Grant
John Sardesai-Grant
Finkelstein, Blankinship, Frei-Pearson & Garber, LLP
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Tel. (914) 298-3292
Fax. (914) 908-6706
Email: jsardesaigrant@fbfglaw.com

Counsel for Lorrell Dumay, Dian Dumay, and Jodi Wolfson.

CERTIFICATE OF SERVICE

I, John Sardesai-Grant, hereby certify that on September 12, 2019 caused the foregoing NOTICE OF APPEARANCE to be filed electronically in the above-captioned action via the Court's CM/ECF system, which caused electronic copies to be served on all counsel of record.

By: */s/ John Sardesai-Grant*

John Sardesai-Grant
Finkelstein, Blankinship, Frei-Pearson & Garber, LLP
445 Hamilton Avenue, Suite 605
White Plains, NY 10601
Tel. (914) 298-3292
Fax. (914) 908-6706
Email: jsardesaigrant@fbfglaw.com

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF QUEENS

----------X Index No. 715629/2019

LORRELL DUMAY, DIAN DUMAY, and
JODI WOLFSON, individually and on behalf
of all others similarly situated,

Plaintiff,

-against NOTICE OF APPEARANCE

EPISCOPAL HEALTH SERVICES INC.,

Defendants.

----------X

To the Clerk of this Court and all parties of record:

PLEASE TAKE NOTICE that Paul M. Sod, 337R Central Avenue, Lawrence, New York 11559, telephone number (516) 295-0707 and fax number (516) 295-0722, does hereby appear in this lawsuit on behalf of the Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson.

Dated: Lawrence, New York
September 16, 2019

s/ Paul M. Sod

Paul M. Sod (PS-9170)
337R Central Avenue
Lawrence, New York 11559
T: (516) 295-0707
F: (516) 295-0722

Counsel for Plaintiffs Lorrell Dumay, Dian Dumay, and Jodi Wolfson

SUPREME COURT OF THE STATE OF NEW YORK COUNTY OF QUEENS

LORRELL DUMAY, DIAN DUMAY, AND JODI WOLFSON, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED.,

Affidavit of Service

Plaintiff(s)

-against-

Index No.

EPISCOPAL HEALTH SERVICES INC.,

Defendant(s)

STATE OF NEW YORK)
)SS.:
COUNTY OF ALBANY)

AUSTIN TAYLOR, being duly sworn, deposes and says: that I am over the age of eighteen (18) years, and reside in Voorheesville, New York;

On September 16, 2019, at 12:08 p.m. I served a SUMMONS, CLASS ACTION COMPLAINT WITH EXHIBITS, AND NOTICE OF COMMENCEMENT, on Defendant, EPISCOPAL HEALTH SERVICES INC., by personally delivering to and leaving with Sue Zouky, a white female approximately 60 years of age, said to be a Business Document Specialist, in the Corporation Division of the Department of State, of the State of New York, at 99 Washington Avenue, Albany, New York, two true copies thereof, and at the same time paid the required fee of Forty and 00/100 ($40.00) Dollars, pursuant to section 306 of the Business Corporation Law of the State of New York.

That deponent, personally knew said Sue Zouky to be a Business Document Specialist, in the Corporation Division of the Department of State of the State of New York, and a person duly authorized to accept service upon the Secretary of State of New York.

Austin Taylor

Sworn before me this
26th day of September, 2019

Notary Public - State of New York

Anne B. Stefanski
Notary Public, State of New York
No. 01ST6369842
Qualified in Albany County
Commission Expires January 22, 2022